Office de la propriété intellectuelle du Canada

Un organisme d'Industrie Canada

Canadian Intellectual Property Office

An Agency of Industry Canada

Bureau canadien des brevets

Certification

Canadian Patent Office

Certification

La présente atteste que les documents ci-joints, dont la liste figure ci-dessous, sont des copies authentiques des documents déposés au Bureau des brevets.

This is to certify that the documents attached hereto and identified below are true copies of the documents on file in the Patent Office.

Specification and Drawings, as originally filed, with Application for Patent Serial No: **2,299,824**, on April 4, 2001, by **SPICER CORPORATION**, assignee of Steven Spicer, Christopher Martin, Steven Coutts, Larry Kuhl, Brian Hollander, Patrick Pidduck, Phillip Von Hatten, Tim Lehan, Mark Onischke and Clayton Grassick, for "Network Resource Control System".

CERTIFIED COPY OF PRIORITY DOCUMENT

L. Lachance

Agent certificateur/Certifying Officer

July 19, 2001

Date

Canada

(CIPO 68)
01-12-00

OPIC CIPO

ABSTRACT

A network resource control system allows network users to communicate with network resources, and includes a resource registry, an administration server, a proxy server, a driver server, and an authorization server. The resource registry includes resource records which are associated with the network resources and define a target address and a resource type for each network resource. The administration server is in communication with the resource registry and provides the resource administrators of each network resource with access to their respective resource records. The proxy server is in communication with the resource registry and facilitates data transfer between the network users and the network resources in accordance with the resource records. The driver server includes driver applications for the network resources. The authorization server is in communication with the resource registry and the driver server and provides the driver applications to the network users in accordance with the resource record. Each driver application includes a resource driver, a driver administrator, and a data transmitter. The resource driver facilitates communication of application data between a user application and target network resources. The resource driver includes a driver input for receiving the application data and a driver output for providing a translation of the application data. The driver administrator is in communication with the resource registry and configures the resource driver in accordance with the resource records associated with the target network resource. The data transmitter is in communication with the driver output and transmits the translated data to the target network resource.

NETWORK RESOURCE CONTROL SYSTEM

FIELD OF THE INVENTION

The present invention relates to a method and system for network management system. In particular, the present invention relates to a method and system for controlling access to network resources.

BACKGROUND OF THE INVENTION

Local area networks are widely used as a mechanism for making available computer resources, such as file servers, scanners, and printers, to a multitude of computer users. It is often desirable with such networks to restrict user access to the computer resources in order to manage data traffic over the network and to prevent unauthorized use of the resources. Typically, resource access is restricted by defining access control lists for each network resource. However, as the control lists can only be defined by the network administrator, it is often difficult to manage data traffic at the resource level.

Wide area networks, such as the Internet, have evolved as a mechanism for providing distributed computer resources without regard to physical geography. Recently, the IPP protocol has emerged as means to control access to printing resources over the Internet. However, the IPP protocol is replete with deficiencies. First, as IPP-compliant printing devices are relatively rare, Internet printing is not readily available. Second, although the IPP protocol allows user identification information to be transmitted to a target resource, access to IPP-compliant resources can only be changed on a per-resource basis. This limitation can be particularly troublesome if the administrator is required to change permissions for a large number of resources. Third, users must have the correct resource driver and know the IPP address of the target resource before communicating with the resource. Therefore, if the device type or the IPP address of the target resource changes, users must update the resource driver and/or the IPP address of the resource. Also, if a user wishes to communicate with a number of resources, the user must install and update the resource driver and IPP address for each resource as the properties of each resource changes. Fourth, access to IPP printers cannot be obtained without the resource administrator locating the resource outside the enterprise firewall, or without opening an access port through the enterprise firewall. Whereas the latter solution provides the resource administrator with the limited ability to restrict resource access, the necessity of opening an access port in the enterprise firewall exposes the enterprise network to the possibility of security breaches.

Consequently, there remains a need for a network resource control solution which allows resource owners to easily and quickly control resource access, which is not hindered by changes in device type and resource network address, which facilitates simultaneous communication with a number of target resources, and which does not expose the enterprise network to a significant possibility of security breaches.

SUMMARY OF THE INVENTION

According to the invention, there is provided a network resource control system and method system which addresses deficiencies of the prior art.

The network resource control system, according to a first aspect of the present invention, allows network users to communicate with network resources, and comprises a resource registry, an administration server, and a proxy server. The resource registry includes resource records which are associated with the network resources and define a target address and a resource type for each network resource. The administration server is in communication with the resource registry and provides the resource administrators of each network resource with access to their respective resource records. The proxy server is in communication with the resource registry and facilitates data transfer between the network users and the network resources in accordance with the resource records.

The network resource control system, according to a second aspect of the present invention, allows network users to communicate with network resources, and comprises a resource registry, a driver server, and an authorization server. The resource registry includes resource records which are associated with the network resources and define a target address and a resource type for each network resource. The driver server includes driver applications for the network resources. The authorization server is in communication with the resource registry and the driver server and provides the driver applications to the network users in accordance with the resource records for facilitating data transfer between the network users and the network resources.

The network resource control system, according to a third aspect of the invention, allows network users to communicate with network resources located behind an enterprise firewall, and comprises a proxy server, and a polling server. The proxy server is located outside the enterprise firewall and receives application data from network users. The polling server is located behind the enterprise firewall and is configured to poll the proxy server for initiating transmission of the received application data from the proxy server to the polling server.

The network resource control system, according to a fourth aspect of the present invention, is associated with a resource registry having resource records associated with network resources for allowing network users to communicate with the network resources, and comprising a resource driver, a driver administrator, and a data transmitter. The resource driver facilitates communication of application data between a user application and target network resources. The resource driver includes a driver input for receiving the application data and a driver output for providing a translation of the application data. The administrator is in communication with the resource registry for configuration of the resource driver in accordance with the resource records associated with the target network resource. The data transmitter is in communication with the driver output for transmitting the translated data to the target network resource.

The network resource control method, according to a fifth aspect of the invention, facilitates communication between network users and network resources, and comprises the steps of:

providing a resource registry including resource records associated with the network resources, the resource records including user access control data;

receiving user access control data from administrators of the network resources for incorporation into the resource records; and

depending upon the user access control data received, configuring the network users for communication with the network resources

The network resource control method, according to a sixth aspect of the invention, facilitates communication between network users and network resources, and comprises the steps of:

receiving a request from one of the network users for communication with a target one of the network resources;

obtaining resource configuration data associated with the target one network resource;

determining a user authorization for communication with the target one network resource; and

depending upon the outcome of the user authorization step, verifying a correspondence between the resource configuration data and user configuration data associated with the one network user.

The network resource control method, according to a seventh aspect of the invention, facilitates communication between users of a network and resources in communication with the network, and comprises the steps of:

providing a request from one of the network users for communication with a target one of the network resources;

receiving from the one network user application data for transmission to the target one network resource, and receiving resource network address data associated with the target one network resource over a communications channel secure from the one network user; and

directing the application data over the network in accordance with received network address data.

The network resource control method, according to an eighth aspect of the invention, facilitates communication over a network between users of the network and network resources located behind an enterprise firewall, and comprises the steps of:

polling a proxy server located outside the enterprise firewall for requests for communication with the network resources;

receiving application data and associated network resource data from the proxy server in response to the poll step; and

directing the application data to the network resources in accordance with associated network resource data.

BRIEF DESCRIPTION OF THE DRAWINGS

The preferred embodiment of the invention will now be described, by way of example only, with reference to the drawings, in which:

Fig. 1 is a schematic representation of a network resource control system, according to the present invention, showing the resource registry, the administration server, the proxy server, the driver server, and the authorization server; and

Fig. 2 is a schematic representation of a driver application for use with the present invention, showing the resource driver, the driver administrator, and the data transmitter.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Turning to Fig. 1, a network resource control system, denoted generally as 100, is shown comprising a resource registry 102, an administration server 104, an authorization server 106, a number of network resources 108, and a number of network users 110. Preferably, each network resource 108 comprises a printing device, and the network resource control system controls access by the network users 110 and the printing devices. However, it should be understood at the outset that the invention is not limited to a network printing control system, and that the network resource 108 may comprise any of a variety of data communication devices, including facsimile machines and image servers.

The administration server 104, the authorization server 106 and the network resources 108 are available by the network users 110 over a wide area network 112, such as the Internet. The resource registry 102 comprises a resource database 114 which includes resource records associated with the network resources 108, and a driver database 116 which includes resource drivers which allow user software applications to communicate with the network resources 108.

Each resource record identifies a target address, resource type and user access level for the associated network resource 108. Also, each resource record identifies a pseudo-name for the associated network resource 108 to identify the network resource to network users. Preferably, the pseudo-name is a network alias that identifies the physical location and properties of the network resource 108, but does not identify the network address of the resource 108. Further, although each network resource 108 may be defined with a unique pseudo-name, a group of network resources 108 may be defined with a common pseudo-name to allow communication with a group of network resources 108.

Preferably, the user access level comprises one of a) "public access" in which any user 110 of the network 112 can communicate with the target network resource 108, b) "private access" in which only members of the enterprise associated with the target network resource 108 can communicate with the target network resource 108, and c) "authorized access" in which only recognized users 110 can communicate with the target

network resource 108. Additional information/restrictions/permissions may also be specified in addition to the foregoing predefined user access levels. For instance, hours of operation, data handling capabilities, and resource pricing may also be specified. Also, restrictions/permissions may be provided either on a per-user basis, or per-group basis.

The administration server 104 provides resource administrators with access to the resource registry 102 to facilitate updating of the target address, resource type, user access level and information/restrictions/permissions identified in the resource records of the resource database 114. In the case of network resources 108 configured for authorized access, the administration server also allows the resource administrators to specify a resource name and password for each network resource 108. As will be appreciated, this mechanism allows the resource administrator to make adjustments, such as to pricing and page limit, in response to demand for the network resources 108, and to make adjustments to restrictions/permissions/passwords to thwart unauthorized access to the network resources 108.

Preferably, the administration server 104 provides controlled access to the resource database 114 so that the resource administrator of a particular network resource 108 is only allowed access to the resource records associated with the resource administrator's network resources 108.

As discussed above, the driver database 116 includes resource drivers to allow user application software to communicate with the network resources 108. As shown in Fig. 2, when a network user 110 is setup to communicate with a target network resource 108 (to be described below), the network communication device of the network user 110 is configured with a driver application 200 comprising a resource driver 202 from the driver database 116, and a wrap-around driver layer 204. The wrap-around driver layer 204 includes a front-end layer 206, an administrator layer 208, and a data transmitter layer 210. The front-end layer 296 is in communication with the network user application software and the resource driver 202, and typically only passes application data from the application software to the resource driver 202. The administrator layer 208 communicates with the resource registry 102 over the Internet 112 and the target network resources 108 to ensure that the driver application 200 is properly configured for communication with the target network resources 108. The data transmitter layer 210 is in communication with the resource driver 202 and is configured to transmit the data output from the resource driver 202 over the Internet 112 to the target network resources 108.

The authorization server 106 is in communication with the resource database 114 and the driver database 116 for providing the network users 110 with the wrap-around driver layer 204 and with the resource drivers 202 appropriate for the target network resources 108. Preferably, the authorization server 106 is configured to provide the data transmitter layer 210 with the network address of the target network resource 108, over a communications channel secure from the network user 110 so that the network address of

the target network resource 108 is concealed from the network user 110. In the case where the network 112 comprises the Internet, preferably the secure communications channel is established using SSL protocol.

Typically, each network resource 108 comprises an IPP-compliant printer. However, as discussed above, other data communication devices, such as facsimile machines, image servers and non-IPP-compliant printers, may be used in addition to or in replacement of an IPP-compliant printer. In the case where the network resource 108 comprises an IPP-compliant device, the network address of the network resource 108 comprises the network resource IPP address. However, in the case where the network resource 108 comprises a non-IPP-compliant device and the network 112 comprises the Internet, preferably the network resource 108 is linked to the network 112 via a server, and the network address of the network resource 108 is the IP address of the server.

Typically each network user 110 communicates to the network resources 108 using a communication device, such as a personal computer, linked to the network 112. However, the network users 110 may also communicate to the network resources 108 using other communications devices, such as wireless telephones, pagers or personal data assistants.

To facilitate communication with network resources 108 located within an enterprise 118 behind the enterprise firewall 120, as shown in Fig. 1, preferably the network resource control system 100 also includes a proxy server 122 located outside the enterprise firewall 120, and a polling server 124 located behind the firewall 120 within the enterprise 118. Preferably, the proxy server 122 is located on-site at the enterprise 118, is provided with a network address corresponding to the enterprise 118, and includes a queue for receiving application data. However, the proxy server 122 may also be located off-site, and may be integrated with the authorization server 106 if desired.

Typically the enterprise 118 includes a server 126 for communication with the network resources 108 located behind the firewall 122. The polling server 124 is in communication with the enterprise server 126 for communication with the network resources 108 located within the enterprise 118. The polling server 124 is configured to poll the proxy server 122 through the firewall 120 to determine whether application data is waiting in the queue of the proxy server 122. However, as will be appreciated, the proxy server 122 and the polling server 124 may be eliminated, if desired, and a port provided within the firewall 120 for communication with the network resources 108 located behind the firewall 120.

Preferably, the network resource control system 100 also includes a transaction server 128 and an archive server 130 accessible over the network 112 via the administration server 104. The transaction server 128 is in communication with the authorization server 106 for keeping track of each communication request between a network user 110 and a network resource 108. For each transmission, typically the transaction server 118

maintains records of the originator, recipient, date, time and file size of the transmission. The archive server 130 is configured to retain copies of the application data transmitted, for a specified period. The network user 110 may specify whether the transmitted application data is to be archived, and the archive period, during a user registration step, described below.

Preferably, the administration server 104 provides controlled access to the transaction server 128 and the archive server 130 so that only the network users 110 which originated transmission of the application data is allowed access to any information associated with the transmission.

To communicate with a network resource 108, preferably the network user 110 first selects a target network resource 108, and configures its computer for communication with the target network resource 108. The network user 110 may also register itself with the administration server 104, by specifying any required information, including the network user's name, physical address, and e-mail address. The network user may also specify that an e-mail notice should be sent to the network user 110 after a successful transmission of application data to the target network resource 108, and whether archiving of the application data is desired. However, the registration step is optional and may be dispensed with if desired.

If no network resource 108 has been selected, the network user 110 queries the administration server 104, via its Internet browser, for a list of available network resources 108. The network user query may be based upon any desired criteria, including print turn-around time and page size (where the target network resource 108 is a printer), price, and geography. In addition, the network user 110 may provide the administration server 104 with the geographical coordinates of the network user 110 in order to determine the network user's nearest network resources. The ability to specify the geographical coordinates of the network user 110 is particularly advantageous if the communication device of the network user 110 is a wireless telephone, pager or personal data assistant. In this latter variation, the administration server 104 may be provided with the network user's geographical coordinates through any suitable mechanism known to those skilled in the art, including latitude/longitude co-ordinates, GPS, and wireless triangulation.

Preferably, a network user 110 will only be provided a list of pseudo-names associated with each network resource 108 satisfying the designated search criteria. Further, typically the pseudo-name list will only identify network resources 108 registered for public access. However, if the network user 110 identifies itself as a registered user by entering a username and password provided at the time of registration, the pseudo-name list will also identify network resources 108 which have been registered for authorized access and to which the network user 110 is authorized to communicate. Also, if the network user 110 is member of an enterprise 118, the pseudo-name list will also identify

network resources 108 which have been registered by the enterprise 118 for private access.

Upon receipt of the resource list, the network user 110 selects a target network resource 108 from the list. The administration server 104 then queries the network user's network communication device to determine whether the communication device has been configured with the appropriate resource driver 202 for communication with the target network resource 108 and, if not, prompts the network user 110 to download the necessary resource driver 202.

Once the network user 108 desires to communicate with a target network resource 108, the network user 110 transmits a communication request via its application software to the driver application 200. The front-end layer 206 of the driver application 200 receives the application data, and passes it to the resource driver 202 for processing. In addition, if the network user 110 has not previously selected a network resource 108, the front-end layer 206 contacts the administration server 104 over the Internet 112 and prompts the network user 110 to select a network resource 108, as described above.

The front-end layer 206 also notifies the administrator layer 208 of the driver application 200 of the print request. The administrator layer 208 then provides the authorization server 106 with a request for printing to a target network resource 108. Typically, the administrator layer 208 provides the authorization server 106 with the pseudo-name associated with the target network resource 108, a network user identifier, and a resource driver configuration identifier. The authorization server 106 then queries the resource registry 102 with the pseudo-name of the target network resource 108 for the associated resource record. The authorization server 106 extracts the user access level from the resource record, and based on the network user identifier, determines whether the network user 110 is still authorized to communicate with the target network resource108. If the network user 110 is still authorized, the authorization server 106 then provides the administrator layer 208 with the network address of the target network resource 108. In the case of a network resource 108 configured for authorized access, the authorization server 106 also provides the administrator layer 208 with the resource name and password associated with the network resource 110.

The administrator layer 208 then queries the network resource 108 over the Internet 112, using the received network address, to determine whether the target network resource 108 still resides at the specified network address, is operational and is on-line. The authorization server 106 also extracts the resource type from the resource record, and based on the resource driver configuration identifier, determines whether the network user 110 is still configured for communication with the target network resource 110. If the network user 110 no longer has the correct resource driver 202, the authorization server 106 queries the driver database 116 for the correct resource driver 202, and prompts the network user 110 to download the resource driver 202. This driver

configuration verification step may be performed concurrently or consecutively with the network address providing step described in the preceding paragraph.

Meanwhile, the resource driver 202 translates the application data into a format suitable for use by the target network resource 108, and then passes the translated data to the data transmitter layer 210 of the driver application 200. Preferably, the data transmitter layer 210 compresses and encrypts the translated application data upon receipt. The data transmitter layer 210 also receives the network address of the target network resource 108 from the driver administrator layer 208, and transmits the compressed, encrypted data over the Internet 112 to the target network resource 108.

If the resource administrator has defined the user access level of the target network resource 108 to allow public access to the network resource 108, preferably the target network resource 108 is accessible through a local server which serves to queue, decrypt and decompress the application data prior to transmission to the target network resource 108. Alternately, the target network resource 108 itself may be configured for transmission over the Internet 112, such as an IPP-capable printer, so that the target network resource 108 prints the application data directly.

If the resource administrator has defined the user access level of the target network resource 108 to allow only private enterprise-based access to the network resource 108, the proxy server 122 located outside the enterprise firewall 120 receives the application data, and transfers the application data to the proxy server queue. The polling server 124 located behind the enterprise firewall 120 periodically polls the proxy server 122 to determine the status of the queue. Upon receipt of a polling signal from the polling server 124, the proxy server 122 transmits any queued application data from the proxy server queue, through the enterprise firewall 120, to the polling server 124. The polling server 124 then parses the network address associated with the received application data, and transmits the application to the appropriate server 126 or network resource 108 for processing.

If the resource administrator has defined the user access level of the target network resource 108 to allow authorized access to the network resource 108, preferably the target network resource 108 is accessible through a local server which serves to queue, decrypt and decompress the application data, and extract the resource name and password transmitted along with the application data. The local server then transmits the application data to the appropriate network resource 108 if the received resource name and password are valid.

Regardless of the user class defined for a network resource 108, if the resource administrator relocates the target network resource 108 to another network address, and/or changes the device type and/or restrictions/permissions of the network resource 108, the resource administrator need only update the resource record associated with the network resource 108 to facilitate communication with the network resource 108.

Subsequently, when a network user initiates communication with the network resource 108 with the original pseudo-name, the authorization server 106 provides the administrator layer 208 with the updated network address of the network resource 108, or prompts the user 110 to download the appropriate resource driver 208, if the network user 110 is still authorized to communicate with the network resource 108.

In the case of network resource 108 configured for authorized access, if the resource administrator desires to change the device name and password associated with the network resource, the resource administrator need only update the device name and password provided on the resource record. Subsequently, when a network user 110 initiates communication with the network resource 108 with the original pseudo-name, the authorization server 106 provides the administrator layer 208 with the updated resource name and password of the network resource 108, if the network user 110 is still authorized to communicate with the network resource 108. A network user 110 who is not authorized to communicate with the target network resource 108, will not receive the updated device name and password from the authorization server 106 and, consequently, will not be able to communicate with the target network resource 108, even if the user 110 knew the network address for the target network resource 108.

The following pages identify further details and benefits of the preferred embodiment.

1OVERVIEW

A mechanism for easily identifying, controlling, and using personal contact information is disclosed. The first embodiment of this method is the support of remote printing devices available through the Internet or internal Intranets is disclosed. A Global Registry is used to control access to and catalog User contact information and Internet Printer Protocol ready printers as well as Proxy enabled standard printers. The invention uses the Global Registry to broker interactions between the users, their contact information, including the available printers. The invention includes the use of a wrapper layer of software around standard O/S print drivers to allow current application technology to be Internet print enabled. The user of the invention is shielded from the complexity and risks of maintaining the current status of those wishing to contact them directly or by printing to a remote printer across the Internet. The providers of the remote printers are shielded from the risks of providing access to their printers and network resources.

2GLOBAL REGISTRY

The Global Registry is a central location on the Web that allows Users to register personal information, including physical location, phone numbers, cell phones, pagers, faxes, internet aware printers and other information. This registered information is protected by passwords, known only to the person registering the information (registrant). The registrant identifies a list of other registrants of the Global Registry that they grant access to, and what aspects, of their personal information that they grant that permission. This permission is also password controlled, and can be limited by factors such as date, elapsed time or access count. The depth and type of information revealed to other registrants can also be controlled on an individual basis. For Instance contact information granted to family members could be different from that granted to co-workers or customers.

The registrant can update the contact information at the central registry whenever any aspect of their contact information changes. These changes are then automatically updated for the other registrants who have been granted access to this information, when they establish contact with the central registry. This gives the registrant a single location to update information, ensuring that those granted permission to contact them, can always get current information.

The first implementation of the method disclosed, is the printerOn System, which is designed to manage and control contact to individuals and organizations through internet enabled printers and fax machines. This same method is applicable to other contact

information such as email addresses, pager numbers, physical location, phone numbers and other information the registrant might wish to share.

3PRINTERON OVERVIEW

3.1 PRINTERON

printerOn is the name of a system of Web based components and drivers that allow current, normal, commercially available Applications to gain controlled, protected printing across the Internet to remote printers. PrinterOn is a sample implementation of the Global Registry method.

3.2 PRINTERON MAIN COMPONENTS

Registration Server - The Registration Server is a Web Server site that supports the registration of Printers and Users as well as the definition of User or Printer groups. It also provides a portal for the provision of advertisement information and sale of merchandise to the registered base of users for any services or products of interest to the users.

Name Server - The Name Server is a Web Server that supports the identification of the appropriate printer IP address for the use of the printerOn Driver and the validation of the User's privileges

PrinterOn Driver - The Driver is a Client Application that looks like a standard device driver that encapsulates the actual printer driver on that O/S, and provides services to route the print stream to Internet Printers.

Proxy Server - The Proxy Server is a Web Server that supports the spooling, encryption and compression of printer data streams to the appropriate printer IP address for the use of the printerOn IPP Print Server.

Global Print Registry - The PrinterOn Global Print Registry is a repository for all of the registered Printers and Users that controls and grants permissions to the users of the system based on the PrinterOn printer settings. The Registry is based on a database model with the accompanying Active Server Pages controlling the transactions.

3.3 PRINTERON REGISTRATION SERVER

The PrinterOn Registration Server supports the registration of both printers and users into the PrinterOn system. The registration of a user consists of entering information such as their Name, e-mail address, real address and the IP identification of their device.

The Registration Server is the main Web interface between Users and the PrinterOn system.

The registration of a printer, consists of identification of the user defined Printer Alias Name, the IP address of the printer, the PrinterOn class of the printer (Public, Authenticated Public, or Private), and if the printer has been identified as Private, who is allowed to print to the registered printer.

3.4 PRINTERON NAME SERVER

The PrinterOn Name Server provides several services to the PrinterOn System in direct communication with the PrinterOn Driver.

In the normal printing process the Name Server would respond to a request for the address of the Printer Alias with a resolved IP address and DNS name for the printer, if it was available to that user. If they were a registered user they could see the Public and Authenticated Public printers in the Registry, filtered as they saw fit. The user could only get a response to a private printer if they were on the list of users associated with that private printer or had access to the printer account and password of the private printer.

3.5 PRINTERON DRIVERS

3.5.1 GLOBAL PRINT DRIVER

The PrinterOn Global Print Driver is a code wrapper that encapsulates a Standard O/S Printer driver with a layer that communicates through a standard Port to the Web. The driver supports the IPP standard protocol and the interaction with the Name Server.

The Global Print Driver is composed of four parts, the Driver Control, the Port Monitor, the IPP printer communication and the IPP print server data stream control.

The novel item is the implementation of a printer driver that passes information through to a Standard O/S Printer driver, while making use of communication with a Website.

A method of controlling the processing or printing requests to a Windows 95, 98 or NT print driver by encapsulating a standard Windows print driver, with a layer that functions as a print driver at the interface, but, allows for control of the print data stream

being passed to windows. This allows for additional processing of the data stream after it has been passed to the driver layer by any Windows application and also the addition of information or redirection of the print driver output from a local printing process to a remote IPP printer.

3.5.2 UNIVERSAL PRINT DRIVER

The PrinterOn Universal Print Driver adds a set of standard O/S Printer drivers built into the driver layer itself, that support the basic data streams for printing to a wide range of printing devices. The idea here is that the printer driver can not only handle control and permissions in a Web environment, but also support printing capabilities to a range of printers without the user needing to install drivers for those printers locally by themselves.

3.6 PRINTERON PROXY SERVER

The printerOn Proxy Server is the provision of IPP services to those users who do not wish to expose their IPP printers outside of a firewall, it also provides services to those who do not have IPP enable printers or servers, but, wish to receive prints over the Internet.

The Proxy server has three components in the design of this subsystem. The first component is an add-on part of the PrinterOn Driver. This part allows for the compression and/or encryption of a data stream in the pass-through printer component of the Global or Universal PrinterOn print drivers.

The second component of the PrinterOn Proxy is a Web location associated with the printerOn.net site that identifies a queue for the printerOn Proxy Printer. The queue is monitored by the printerOn Print Server and if data appears in the queue, the Server initiates a download of the data from behind the firewall, at the printer location. This solution means that Administrators can provide the services of an IPP printer without opening a port through the Firewall of their network.

The third component of the printerOn Proxy is the printerOn Print Server that is located at the site of the Proxy Printer. This server supports the decryption and expansion of the data stream being spooled from the Proxy Queue and then passes this to the printer connected to the server. This means that data streams that are IPP compliant as well as others may serviced by printing devices that do support the IPP capabilities.

3.7 REGISTRY

3.7.1 GLOBAL PRINT DRIVER REGISTRY

The Global Print Registry is the database of registered Printers and Users that comprise the printerOn system. The level of indirection provided by this registry allows for the insertion of many services and capabilities not supported by standard IPP printers or other Internet printing solutions. The use of both User and Printer Aliases means that the actual physical connection or the physical device behind that alias can be moved, reconfigured or changed without changing the appearance of the alias at the user level. The Administrator of the system can modify and maintain a distributed group of printers over the Internet, simply by accessing the single registry location. The use of the alias also ensures that the publication of the address on a website, business card or directory is a viable alternative as the alias is controlled and mapped to the changing network underneath. Even physical location can be easily changed. This means that printing can work at the same virtual portal style that users have come to expect from browser access to the Web.

The use of printer IDs and user Ids in the system, in conjunction with passwords, means that the use of the internet printers can be controlled, and modified from the same central registry.

4PRINTERON PROCESS DISCUSSION

4.1 REGISTERING A PRINTER

4.1.1 REGISTRATION OF AN IPP PRINTER

PrinterOn as a system is centered around the internet printer. Unlike standard systems that focus on the user and permissions PrinterOn is unique in that it is printer centric. The printer is given an identification and is registered in a central registry, with a level of security and if necessary, a list of users that may be granted permission by the printer itself, to use the printer. This is a unique level of active security to control the use of the printers. To accommodate this level of security, printers that have an IPP interface must be registered within the PrinterOn system. This registration is entirely in the control of the Administrator of the printer, both in initiating the registration and in maintaining the nature and type of printer at that location.

00/02/00 20:02 FAX [illegible] [illegible] [illegible]

If the user has a printer that does not have an IPP Server or is not enabled with IPP technology, the printerOn system provides the ability to provide an IPP Proxy for connected printers. If the user registers a printer and identifies it as a non-IPP printer, the printerON.net site can provide a printing queue to store and process data transmitted across the internet. If users of the printerOn system print to that printer the Proxy services in the printerOn Print Driver are enabled and the data is known to be being transmitted to a non-IPP printer and is routed to the printerOn.net site. From there the data is queued and sent on to a printerOn Proxy print server located at the non-IPP printer's location. This Print Server then formats the data stream and forwards the information to the printer.

11.0.2 PRINTER GROUPS

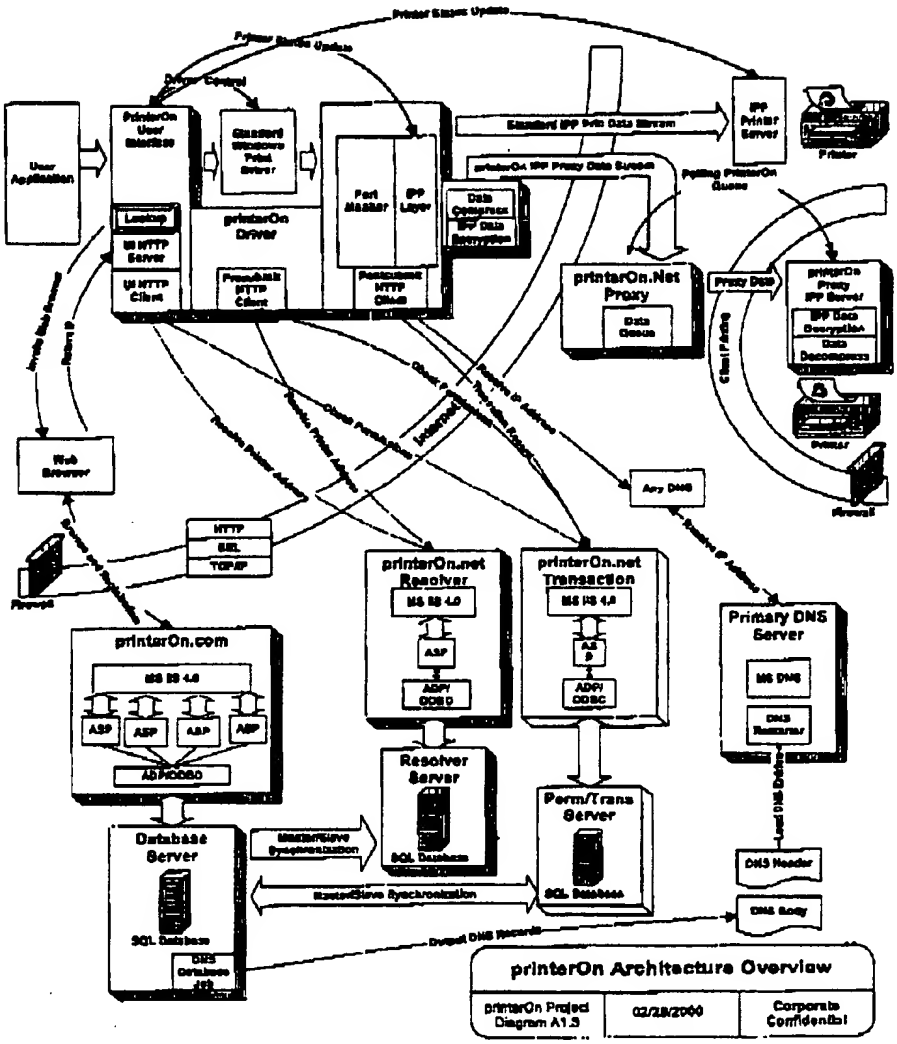
The printerOn.com interface allows for the registration of a Group of Registered Printers. This Printer Group consists of a series of printers that have been registered in the Global Print Registry associated and given an Alias by the User. This grouping of Registered Printers gives the user of the system the ability to print to a set of IPP Printers simultaneously, through their standard printing interface. The user simply identifies the printerOn Printer Group as their printer in their application printing dialog, and the resultant print is sent to all of the Registered Printers in that group.

If the Group of Registered Printers includes Fax locations, those faxes will be simultaneously sent along with the prints to the appropriate fax machine. This means that printers and faxes can be mixed within a single information exchange. If there are several fax locations, these can be routed to a fax distribution center for further forwarding to the actual fax devices.

11.0.3 REGISTRANT GROUPS

The printerOn.com interface also allows for the registration of a Grouping of Registrants. This would enable work groups or company divisions to identify a group of people that could as a class, be granted access permission to a given Private Printer.

PrinterOn Overview



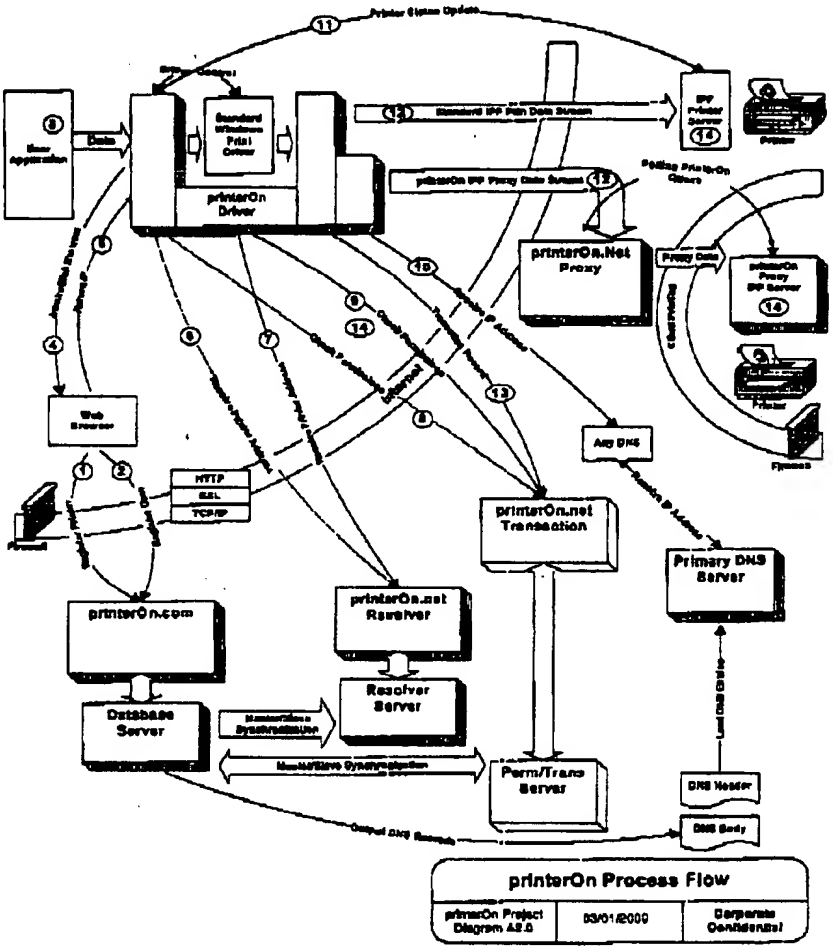
11.1 REGISTERING A USER

The users of the printerOn system must register with the Global Print Registry to ensure that they can use the full features of the printerOn system. Users log onto the printerOn.com website and enter the User Registration information to ensure the printerOn system can recognize them and identify which printing capabilities are available to them. If Users do not register, then they can only use the Public Printers listed in the registry. Once the users have registered they are considered to be Registrants in the printerOn system and can have access to Authenticated Public printers and those private printers that they have been granted access to.

The data captured during the printerOn Registration of a User such as:

- A unique User Registrant identifier
- A Registrant name
- An address
- A valid email address
- An assigned Registrant password, emailed to the above address.
- Default printerOn settings
- A fax alias
- A phone number

PrinterOn Process Flow



5

8.1 FINDING A PRINTER

8.1.1 WHEN PRINTING

When the user identifies that they wish to print from an application using the printerOn driver, the can either identify the printer from their favorites list, type in the Printer Alias or invoke the Search Browser to look for a printer in the Global Print Registry.

Once the user has identified the printer they wish to use, the printers characteristics are checked to determine if the user has a printer driver for that device, if the printer is online through an IPP status check and if the user has permission to print to that device.

If the user has the appropriate driver and permission, the printerOn Printer will become the default printer for that application and workstation, ready for printing.

For Registrants of the printerOn system who wish to use advanced search techniques during a printing job searches can be done by available printer types, geographic location, delivery capability, job quality or by a reverse bidding process. This reverse bidding process consists of comparing Registered Printer capabilities and pricing with the Registrants request for services and providing the Registrant with a best fit solution.

8.1.2 WHEN ONLINE TO PRINTERON.COM

When the user is accessing printerOn.com they have the ability to search for printers available to them, they can search either geographically, by printer model or by printer type and permissions.

The user also has the ability to undertake the same advanced searching techniques for printing resources that are available from the printerOn Driver interface. These can involve determination of the best price for a printing job, the closest geographic location, perhaps fastest delivery or closest match to the required capabilities.

Once they have located a printer, they can choose to add this printer to their List of Favorites in the printerOn Driver.

8.2 PRINTING A DOCUMENT

When the user is printing from an application, they can use the default selection or choose a new printer from their favorites or browse the printerOn.net website for a printer in the Global Print Registry.

Once a printer has been identified the printer IP address is communicated in an encrypted message to the printerOn Driver and the user may print to this Remote Printer. When the print is initiated the printerOn driver will communicate with printerOn.net to ensure that the permissions and printer status and location are valid.

If the response to the communication indicates that the printer has been changed, the printerOn driver will check the local system for an appropriate printer driver for the newly installed printer. If it is not available then the printerOn driver will request a copy of the appropriate driver from printerOn.net. If the printer driver is not available at the printerOn.net site, the printer Administrator will be notified and the Registrant will be asked to find a copy of the appropriate driver. If the driver is available, then the printerOn Driver will download it to the Registrants machine and continue with the printing request.

The printerOn Driver then allows the data stream from the application to pass-through to the printer model device driver for processing. Once this is completed the printerOn driver then gets the data stream from the driver and packages it up into an IPP data stream or a Proxy data stream for a non IPP printer. The IPP layer of the printerOn driver then initiates an IPP session with the actual remote printer confirms it's status and sends the data. The driver then in parallel, sends a transaction record to printerOn.net to record the printer usage and statistics such as number of pages, transmission time and other statistics for accounting and administration purposes.

9IDENTIFIED VERTICAL MARKET APPLICATION FOR PRINTERON

9.1 OVERVIEW OF APPLICATIONS

- Universal Use – The Universal use applications are those that are generally applicable to all printing applications.
- Wireless Applications – The Wireless applications are those services and capabilities that enhance the use of wireless devices. Such as interactive pagers or cell phones

- Fax Substitution – The Fax Substitution is the provision of services that will supplement or replace the normal fax transmission process.

- IPP Server Enhancement – The IPP Server Enhancement applications are services and capabilities that expand the use and function of the IPP standard printers.

- Reprographics – The Reprographics applications are those that enhance the commercial printing and services market.

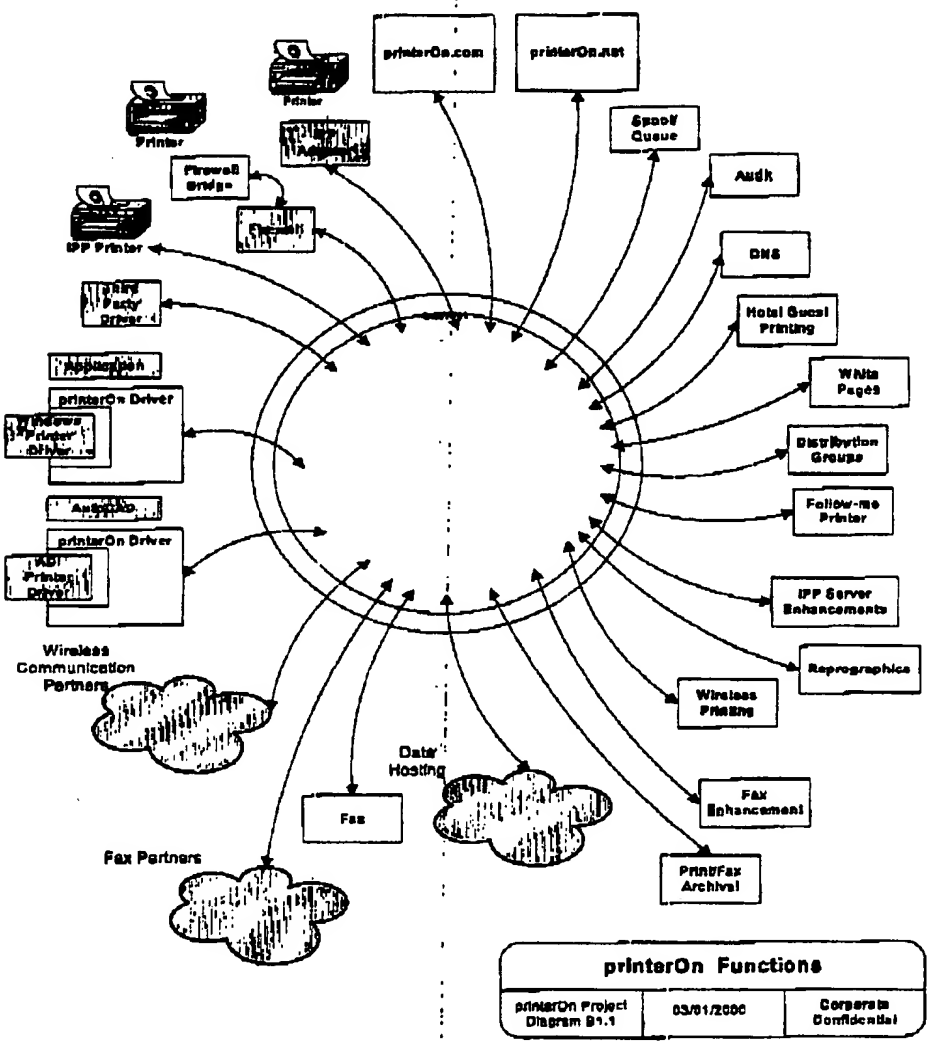
5.1 UNIVERSAL USE

5.1.1 HOTEL GUEST PRINTING

For business travelers who need printed data, but do not bring printers with them, hotels can register an IPP printer with printerOn.net. When a guest arrives at the hotel, he or she can be assigned a valid printerOn userID and password by a Printer Administrator at that Hotel through the printerOn.com Website, that will allow access to the hotel printer for the duration of the guest's stay. printerOn will broker access to the printer in such a manner that it remains secure. printerOn can provide the hotel with the option of tracking printer usage for guest billing purposes. Guests can print from their rooms through dial-up internet connections using printerOn.net, and pick up their output at the front desk. If they wish they can also print a cover page on each of their print jobs, identifying who the print is to go to.

Once the guest has been registered with printerOn.com their access to the printer will be automatic for the duration of the configured access. The printerOn driver will substitute the password for the printer into the print request from the guest's application. The hotel can then get a record of the guest's printing activity for billing purposes.

PrinterOn Vertical Markets



5

5.1.2 WHITE PAGES

printerOn.net will act as a search engine for IPP print addresses, allowing users to always locate the appropriate device even as servers and printers are being replaced or moved. Organizations can update the parameters for registered printers at printerOn.net to minimize disruptions in service for those authorized to access their printers. This means that system administrators can reconfigure or replace physical printers, while retaining the permissions, passwords and Printer Aliases for the Registrants. The Registrants will not necessarily even be aware that the physical printer that they use has been changed.

5.1.3 DISTRIBUTION GROUPS

printerOn allows the creation of a logical Printer Group, so that users can send a copy of a document to a number of people or printers in one step. By printing to the group, a copy of the printout is automatically duplicated by the printerOn Print Driver by recursively printing and sending to each device belonging to the group. The standard Print Driver needed to print to each member of the group will be detected and inserted as in the single device printerOn process.

5.1.4 PAID-FOR-PAPERS

printerOn.net can broker physical prints of an organization's purchased reports directly to a consumer's output device, saving the time and cost of shipping hardcopy versions. There is no intermediate electronic form that may be copied, and the report is available immediately.

The provider of the reports, can request the IP address of the customers printer, or ask that the customer register the printer as Private. Then the provider can print to the printer, with a record of the transaction being available to show delivery.

If the person requesting the print wishes, they can have the print stream information forwarded to a local printing shop to be picked up or forwarded.

5.1.5 PRINT/FAX ARCHIVAL

For clients who require records of faxes or IPP prints, but lack document archival software, printerOn.net can host a copy of print jobs for a period of time. The prints

can be regenerated or retrieved on demand by those with suitable password access. printerOn.net will also work closely document management companies to provide similar capabilities for larger organizations with a higher degree of IT strategy. This capability can be supported by the printerOn system, because the printerOn driver is capable of producing multiple renditions of a single print request, one of which can be routed to an archival process.

5.1.6 FOLLOW-ME PRINTER

Registering with printerOn ensures that faxes or prints always reach recipients who change their locations. Corporations can be certain that output will find traveling, former, or vacationing employees, and can also redirect prints for absent employees to suitable alternates. An individual registers a virtual IPP address with printerOn. This virtual IPP address is the one they expose to the world. As they change locations, as the Administrator of their printer, they can visit the printerOn Web site and redirect their virtual IPP device to the IP address of the physical print device at their current location.

5.2 WIRELESS APPLICATION

5.2.1 PRINTING WIRELESS EMAIL

For business travelers who receive e-mail, printerOn will have integrated solutions with wireless data services that allow the recipient to print a copy of the message on an IPP printer. The wireless user can specify the printer they want to use, or can rely upon printerOn services to locate a suitable printer based upon geographic location and other requirements. Geographic location may be established by several means, including GPS, wireless cell triangulation, or manual entry.

5.2.2 OBTAINING EMAIL ATTACHMENTS

E-mail attachments can be printed directly to printers rather than opened in the programs they were created in. Wireless devices, such as Internet-enabled cell phones and wireless modems or pagers, can thus alert the user of a received attachment without needing to deliver the contents to the device. The business traveler can request that the e-mail be forwarded to printerOn.net with a request to output the message and attachment on a hardcopy printer. This hardcopy may be a fax machine, public, private or Virtual IPP printer. printerOn will also be able to obtain the geographic coordinates of a wireless device either from a GPS or cell phone locating service to

automatically route the prints to the nearest printer, or provide the user with a list of nearest printers to choose from.

5.3 FAX SUBSTITUTION

5.3.1 IMPROVED FAXING

printerOn.net can replace faxes, with high quality prints that retain fine details traditionally lost using fax machines. An IPP printer can be registered along with the fax number(s) for which it is a substitute. Clients can cross-reference these fax numbers (which are commonly available) into IPP print addresses to send high quality fax-equivalents to business partners. printerOn.net is capable of determining when a fax number does not have an IPP equivalent, and dropping into standard fax mode under these circumstances.

If numerous real fax locations are identified, then faxes can be routed to a fax distribution center for forwarding.

5.4 IPP SERVER ENHANCEMENT

5.4.1 IPP PRINTER ADAPTER

printerOn can create virtual IPP printers for companies whose printers are not IPP compliant, or who lack the expertise to set up an IPP device. Corporations receive an application that runs on their Windows NT, 2000, or Linux print servers that allows a printer to behave as a virtual IPP printer when used in conjunction with printerOn.net. This application communicates with the printerOn Web site to convert IPP print requests from any source into a print request for non-IPP printers.

5.4.2 PEN MAPPING

The printerOn Driver creates a definition table to map the data stream being presented to the Print Driver Interface to any of several standard or custom definitions. This means that the color of the objects can be mapped to other colors or grayscale, the thickness of lines can be mapped, the fill patterns used can be modified or mapped to color or grayscale fills. In the printerOn system, because the driver knows the capability of the final printing device, the printerOn driver can automatically map the data input from the Application to an appropriate output stream for that printing device, without any modifications or intervention with the originating Application. If the printing device is a black and white

printer, colors can be mapped to grayscale fills or patterns. If the resolution of a printer is less than the original data, then fill patterns can be modified to accommodate the lower resolution.

5.4.3 IPP FIREWALL BRIDGE

For companies with security concerns over "pushing" data through their firewalls, printerOn can expose a printer without opening a port in the firewall. This is accomplished by an application on the company's server that "polls" the printerOn service to identify when a print request has been made. It then pulls that data securely through the firewall, rather than allowing it to be pushed through.

5.4.4 IPP DATA OPTIMIZATION

To decrease the use of expensive or slow Internet bandwidth, printerOn offers a service/product combination that will optimize data transfer for IPP print applications. The printerOn driver can compress the print data stream before transmission. printerOn software on the receiving IPP server performs complementary decompression to provide the necessary print data to the printer. The printerOn driver will "handshake" with the print server to establish if this service is available on the printer, and automatically use it when appropriate.

5.4.5 IPP DATA QUEUING

To reduce printing bottlenecks caused by slow Internet connections or large print jobs, the printerOn Proxy provides a service in which the printerOn.net Web site can respond with a "ready" signal to anyone wanting to print to an IPP printer. printerOn will then queue the data and ensure transmission of the print request once the printer becomes available.

5.4.6 IPP DNS

For smaller organizations requiring Domain Name Server support (a requirement for remote printer access), printerOn.net will act as a global DNS. This will simplify the process and reduce the cost of exposing IPP printers for the average company lacking the technical expertise or the financial rationale for building a DNS.

5.4.7 PRINT IDENTIFICATION

To provide some context for the print transaction, printerOn can either place header text on the printed document or produce a cover sheet to identify the source and destination of the document. This print header or cover sheet can include information such as the time, date, who printed the document, and who is expected to receive the document.

5.4.8 PRINT AUTHENTICATION

printerOn can verify the authenticity of a print submission through passwords, public key encryption, and other accepted security mechanisms. This further reduces the reliance on courier and fax transmission as a means of validating transactions. A recipient of a print job is able to check document validity according to the printerOn.net registry. Reprints on demand of authenticated documents are retained for a period of time, and audit trails are available permanently.

5.4.9 PRINTER ACCOUNTING

To help organizations monitor consumables and track costs among departments, printerOn.net can record all printer activity by user, account code, and printer. Customized reports for auditing purposes can be generated, unusual print behaviors flagged, and e-mail notifications can be sent to a designated contact when supplies need checking.

5.4.10 PRINTER USE PRIORITIZATION

Critical documents can be printed first, rather than be delayed by long print jobs or slow data transfer. The printerOn system allows the printer owner to identify printerOn users to whom they wish to give priority access. A print request from such a user that is identified as being high priority will be given preference for next servicing, or may even terminate (pre-empt) the current print job depending upon the printer owner's configuration.

5.4.11 PAPER SIZE FILTERING

To ensure that the correct paper size for the remote printer is selected by users, the owner of the registered printer can identify to printerOn what page sizes are valid (as opposed to what page sizes are technically possible). Typically, these are the sizes that are actually installed in the device. When printing from the printerOn driver, we will ensure that the user has constrained their paper selection to a valid size to prevent this condition from occurring. Alternatively, printerOn can automatically scale (or resize) the print job so that it fits on the available paper.

Note that similar applications exist for media (paper, vellum, mylar etc), color/black and white printing, and folding (staples, punches, fold type, etc.).

5.4.12 AUTOMATIC PRINT DRIVER VALIDATION

printerOn will ensure that the printer and printer driver are compatible, and will thereby prevent the user from producing incorrect output. To guarantee this, the Global Print Registry allows anyone to search for a printer to discover its type, so they can install or use an appropriate print driver. Furthermore, if you use the printerOn driver, the system will automatically check the currently selected print driver against the global registry database, either to provide a warning of incompatibility, or to entirely block the print attempt.

5.4.13 NOTIFICATION AND RECEIPTS

To eliminate uncertainty, printerOn can assure the sender that the document printed successfully, and can inform the recipient that a document has arrived at their printer. The system can be configured to allow or enforce the generation of print e-mail notifications and receipts. Typically, these messages would contain information such as the physical location and URL of the printer, the number of pages, who printed it, and for whom it was printed.

Upon completion of a print, the print monitor will interact with the printerOn audit site to record the statistical data related to the print job. The audit site is capable of creating e-mail notifications and receipts incorporating this statistical data. The user may request a receipt in the print driver user interface, or may choose to always obtain a receipt if they have configured their account appropriately. A recipient notification is generated if the user has entered the e-mail address of the recipient in the print driver. A printer owner can configure their account such that they always receive notification, or receive notification in the event that an explicit notification was not requested.

5.4.14 CONFIGURATION-PROOF PRINTER NAMING

To guarantee the long-term validity of a URL address while allowing printer owners the freedom to change printer paths, printerOn.net allows owners to create an alias for a logical printer. This alias remains valid despite changes to a host domain, servers, printers, or server configuration. Users of printerOn.net and the printerOn driver are shielded from configuration changes, allowing printer administrators the freedom to modify their environment without impacting published URL printer names.

5.4.15 PRINTER DENIAL

For companies concerned about receiving unsolicited information ("spam") or the inappropriate use of equipment, (printing hate messages, pornographic images, etc), printerOn allows the printer owner to track or block this type of behavior. One such method is to restrict access to the printer only to registered printerOn users. This provides a mechanism for tracking inappropriate print users, which discourages poor behavior. Another unique printerOn concept is the ability to grant access on a "denial" basis. Most access granting protocols identify who is allowed to use a service (printerOn supports this model). We also provide a means of controlling access to a printer that says "anyone can use the printer EXCEPT for the following users...". This is important since IPP printers provide a new problem for printer administrators... the environment is no longer controlled (as in a corporation). Rather, it is the world at large.

5.5 REPROGRAPHICS

5.5.1 LARGE FORMAT PRINT JOB SUBMISSION

The printerOn driver can assemble print jobs from the Application printing process and apply the appropriate Printer Job Control wrappers, depending on the nature of the target printer. If the choice of output location involves the use of a different printer manufacturers control environment, then the printerOn driver can use a different set of Job Control codes to match the selected remote output device, without user intervention.

5.5.2 PRINTING AND COPY SHOPS

Small print shops, can register a secure public IPP printer with printerOn.net to serve customers who lack the equipment or skills to print their specialized documents. The customer can then obtain the hardcopy results from the print shop. The customer would contact the Print Shop, who tells them to use printerOn with a time limited UserID and Password. The customer prints using the printerOn driver on their desktop, which interacts with printerOn.net to validate and provide a temporary access to the Print Shop IPP printer. Once the print job is complete, the access expires.

5.6.3 PRINT FORWARDING

An application for the remote printing job, is to produce hardcopy output at a site with good availability to the final destination, if that destination does not have an IPP printer. This means that documents could be printed remotely to a printing establishment near a courier hub site. The courier can distribute the resultant hardcopy, without the necessity of picking up the hardcopy and bringing into the hub. It would be printed and distributed from that hub.

The foregoing description is intended to be illustrative of the preferred embodiment of the present invention. Those of ordinary skill may envisage certain additions, deletions and/or modifications to the described embodiment which, although not explicitly described herein, are encompassed by the spirit or scope of the invention, as defined by the claims appended hereto.

WE CLAIM:

1. A network resource control system for allowing communication over a network, between network users and network resources, the network printing system comprising:

a resource registry including resource records associated with the network resources, the resource records defining a target address and a resource type for each said network resource;

an administration server in communication with the resource registry for providing administrators of each said network resource with access to respective ones of the resource records; and

a proxy server in communication with the resource registry for facilitating data transfer between the network users and the network resources in accordance with the resource records.

2. A network resource control system for allowing communication over a network, between network users and network resources, the network printing system comprising:

a resource registry including resource records associated with the network resources, the resource records defining a target address and a resource type for each said network resource;

a driver server including driver applications for the network resources; and

an authorization server in communication with the resource registry and the driver server for providing the driver applications to the network users in accordance with the resource records for facilitating data transfer between the network users and the network resources.

3. A network resource control system for allowing communication over a network, between network users and network resources located behind an enterprise firewall, the network printing system comprising:

a proxy server provided outside the enterprise firewall for receiving application data for printing; and

a polling server provided within the enterprise, the polling server being configured for polling the proxy server for initiating transmission of the received application data from the proxy server to the polling server.

4. A network resource control system for allowing communication over a network, the network printing system being associated with a resource registry including resource records associated with network resources for allowing network users to communicate with the network resources over the network, the network printing system comprising:

a resource driver for facilitating communication of application data between a user application and target ones of the network resources, the resource driver including a driver

input for receiving the application data and a driver output for providing a translation of the application data;

a driver administrator in communication with the resource registry for configuration of the resource driver in accordance with the resource records associated with the target one network resources; and

a data transmitter in communication with the driver output for transmitting the translated data to the target one network resources.

5. A method for facilitating communication over a network, between network users and network resources, comprising the steps of:

providing a resource registry including resource records associated with the network resources, the resource records including user access control data;

receiving user access control data from administrators of the network resources for incorporation into the resource records; and

in accordance with the user access control data, configuring the network users for communication with the network resources.

6. A method for facilitating communication over a network, between network users and network resources, comprising the steps of:

receiving a request from one of the network users for communication with a target one of the network resources;

obtaining resource configuration data associated with the target one network resource;

determining a user authorization for communication with the target one network resource; and

in accordance with the user authorization, verifying a correspondence between the resource configuration data and user configuration data associated with the one network user.

7. A method for facilitating communication over a network, between network users and network resources, comprising the steps of:

providing a request from one of the network users for communication with a target one of the network resources;

receiving from the one network user application data for transmission to the target one network resource, and receiving resource network address data associated with the target one network resource over a communications channel secure from the one network user; and

directing the application data over the network in accordance with received network address data.

8. A method for facilitating communication over a network, between network users and network resources located behind an enterprise firewall, comprising the steps of:

polling a proxy server located outside the enterprise firewall for requests for communication with the network resource;

receiving application data and associated network resource data from the proxy server in response to the poll step; and

directing the application data to the network resources in accordance with associated network resource data.

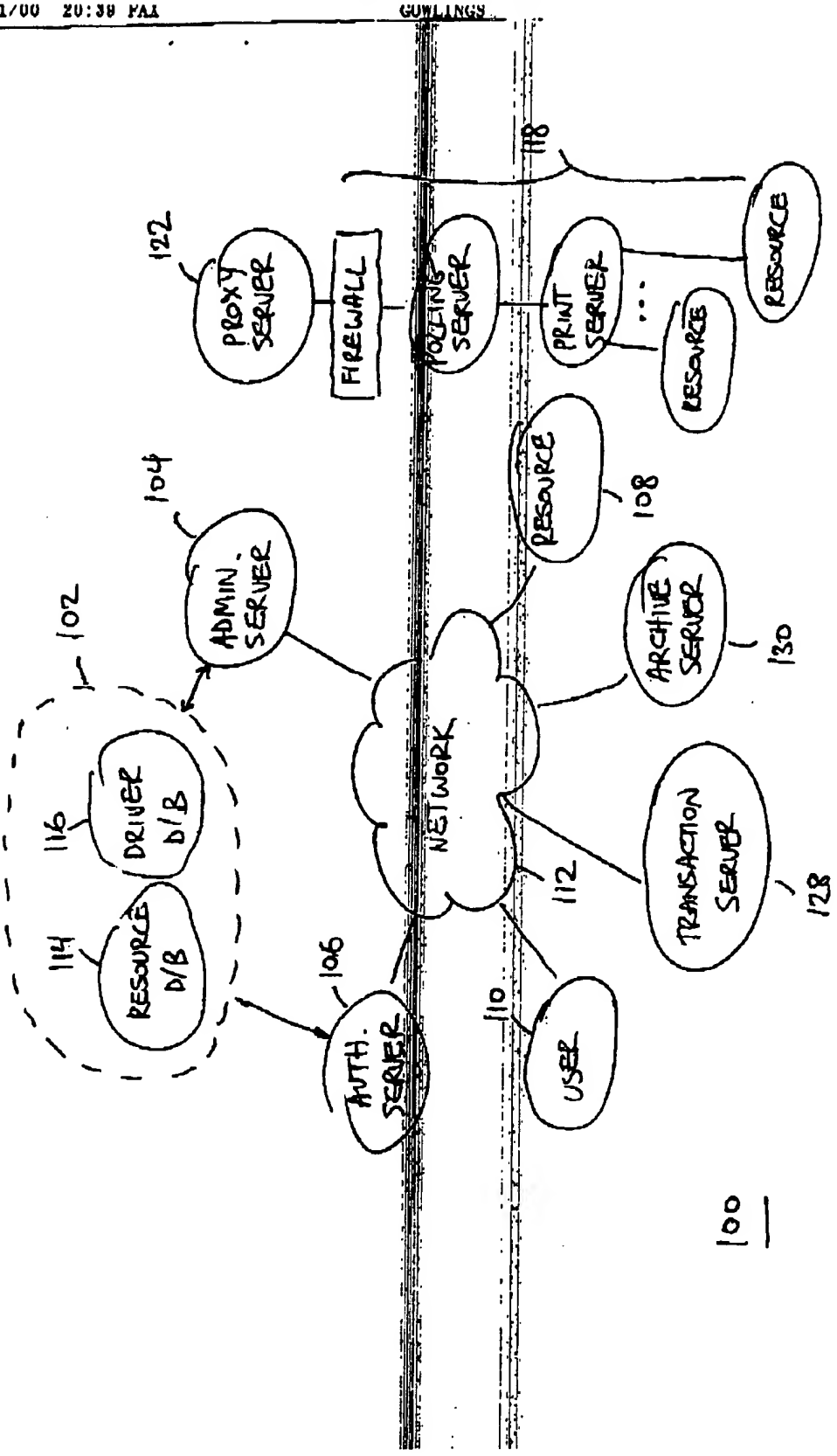
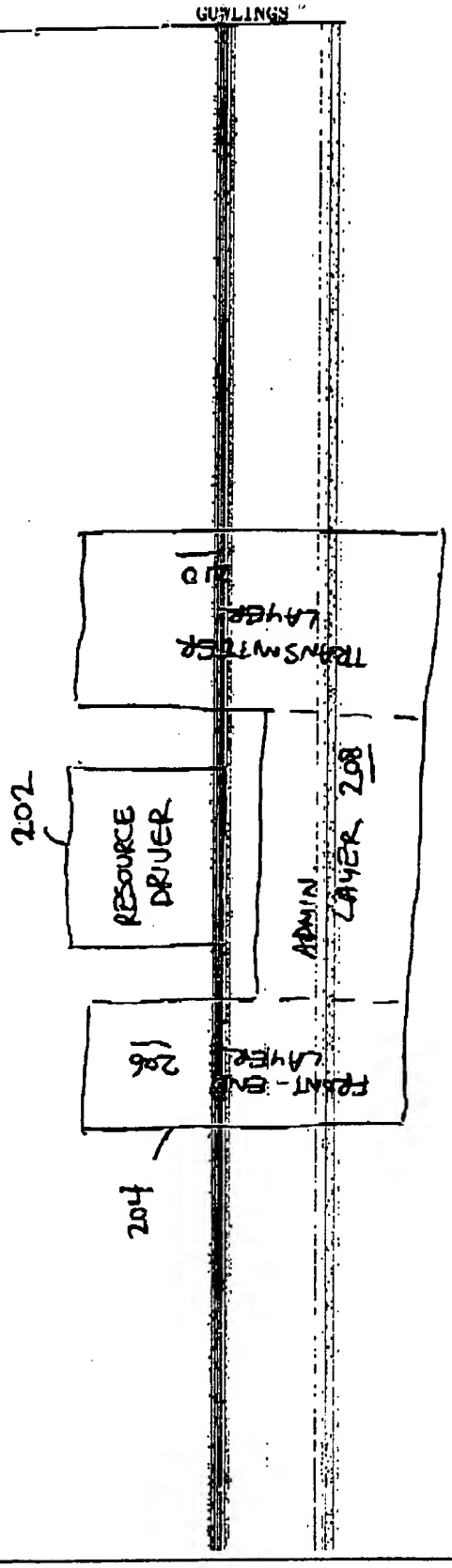

100
102
104
106
108
110
112
114
116
118
122
128
130
ADMIN. SERVER
AUTH. SERVER
DRIVER D/B
RESOURCE D/B
NETWORK
USER
RESOURCE
PROXY SERVER
FIREWALL
ROUTING SERVER
PRINT SERVER
RESOURCE
RESOURCE
ARCHIVE SERVER
TRANSACTION SERVER

FIG. 1


TRANSMITTER LAYER
210
RESOURCE DRIVER
202
ADMIN LAYER 208
FRONT-END LAYER
206
204

200

FIG. 2